ANONYMOUS

Proposal and Comment Information

Title: Proposed Third-Party Risk Management Guidance, OP-1881

Comment ID: FR-2026-0031-01-C02

Submitter Information

Name: Anonymous

Submitted Date: 09/13/2026

PUBLIC COMMENT SUBMISSION
To: Commodity Futures Trading Commission
Re: Request for Information — Proposed Third Party Risk Management Guidance
Docket: OCC Docket ID OCC-2026-0793 / Federal Reserve Docket OP-1881
Submitted by: Bilal Ali Zafar
Title: Manager, Risk Management
Organization: National Industrialisation Company (TASNEE), Riyadh, Saudi Arabia

I submit this comment to the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and National Credit Union Administration:

I appreciate the opportunity to comment on the proposed Third-Party Risk Management Guidance.

I am a risk and governance professional with more than seventeen years of experience across financial services and complex operating environments, with professional responsibilities spanning enterprise risk management, compliance, internal controls, operational resilience, business continuity, governance, and third-party risk management.

I support the agencies' movement toward a more principle based and proportionate approach to third party risk management. In particular, the proposed emphasis on assessing both the magnitude of potential harm and the likelihood of occurrence, rather than automatically subjecting broad categories of third parties to identical levels of oversight, should help institutions direct risk management resources toward relationships capable of producing material financial, regulatory, operational, or customer impacts. The proposal appropriately recognizes that third party relationships do not present uniform levels of risk and that risk assessments should reflect an institution's circumstances.

I respectfully recommend, however, that the final guidance strengthen several areas.

First, third party risk assessment should explicitly consider aggregated dependency and concentration risk. Assessing individual relationships in isolation may produce a reasonable risk rating for each vendor while failing to identify a material concentration across several critical business services. For example, multiple applications, business units or customer services may ultimately depend upon the same cloud provider, core processor, data infrastructure, geographic location, subcontractor or technology platform. Accordingly, banking organizations should be encouraged to evaluate third party risk at two levels: the individual relationship level and the enterprise portfolio level. Portfolio level assessment would enable management and boards to identify single points of failure, correlated dependencies and concentrations that may not be apparent through individual vendor assessments alone. The proposal already acknowledges that reliance on a third party for extensive services can create concentration risk; expanding this principle into an enterprise view would further strengthen resilience.

Second, the agencies should provide a non-prescriptive set of risk characteristics that institutions may consider when determining whether a relationship warrants heightened oversight. Such characteristics could include the potential impact on customers or critical operations, access to sensitive information or systems, regulatory exposure, substitutability of the provider, concentration and dependency, use of material subcontractors, financial viability of the provider, recovery capability, and the potential scale of operational disruption. This should remain illustrative rather than become a mandatory checklist. The objective should be to improve consistency of risk judgment without recreating the process driven approach the proposed guidance is seeking to correct.

Third, third party risk assessment should be dynamic rather than primarily calendar driven. The proposed guidance appropriately recognizes that changing circumstances may justify reassessment of a relationship. I recommend that the final guidance further encourage event driven reassessment where there is a significant cyber incident, material control failure, regulatory action, financial deterioration, major change in service scope, significant subcontractor change, acquisition, geopolitical exposure, prolonged service interruption, or material change in concentration. Such an approach would permit institutions to devote monitoring resources to changes in actual risk rather than relying principally on uniform annual reassessment cycles.

Fourth, operational resilience should form an integral part of higher risk third party assessment. I support the proposal's recognition that resilience arrangements, alternative providers, segregated data backups, and demonstrated recovery capability may materially reduce the consequences of disruption. For relationships supporting important operations, institutions should consider whether recovery capabilities have been demonstrated through testing rather than relying exclusively on documented continuity plans. Where practical, assessments should consider recovery objectives, service

PUBLIC COMMENT SUBMISSION

To: Commodity Futures Trading Commission
Re: Request for Information — Proposed Third Party Risk Management Guidance
Docket: OCC Docket ID OCC-2026-0793 / Federal Reserve Docket OP-1881

Submitted by: Bilal Ali Zafar
Title: Manager, Risk Management
Organization: National Industrialisation Company (TASNEE), Riyadh, Saudi Arabia

---

I submit this comment to the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and National Credit Union Administration:

I appreciate the opportunity to comment on the proposed Third-Party Risk Management Guidance.

I am a risk and governance professional with more than seventeen years of experience across financial services and complex operating environments, with professional responsibilities spanning enterprise risk management, compliance, internal controls, operational resilience, business continuity, governance, and third-party risk management.

I support the agencies' movement toward a more principle based and proportionate approach to third party risk management. In particular, the proposed emphasis on assessing both the magnitude of potential harm and the likelihood of occurrence, rather than automatically subjecting broad categories of third parties to identical levels of oversight, should help institutions direct risk management resources toward relationships capable of producing material financial, regulatory, operational, or customer impacts. The proposal appropriately recognizes that third party relationships do not present uniform levels of risk and that risk assessments should reflect an institution's circumstances.

I respectfully recommend, however, that the final guidance strengthen several areas.

First, third party risk assessment should explicitly consider aggregated dependency and concentration risk. Assessing individual relationships in isolation may produce a reasonable risk rating for each vendor while failing to identify a material concentration across several critical business services. For example, multiple applications, business units or customer services may ultimately depend upon the same cloud provider, core processor, data infrastructure, geographic location, subcontractor or technology platform. Accordingly, banking organizations should be encouraged to evaluate third party risk at two levels: the individual relationship level and the enterprise portfolio level. Portfolio level assessment would enable management and boards to identify single points of failure, correlated dependencies and concentrations that may not be apparent through individual vendor assessments alone. The proposal already acknowledges that reliance on a third party for extensive services can create concentration risk; expanding this principle into an enterprise view would further strengthen resilience.

Second, the agencies should provide a non-prescriptive set of risk characteristics that institutions may consider when determining whether a relationship warrants heightened oversight. Such characteristics could include the potential impact on customers or critical operations, access to sensitive information or systems, regulatory exposure, substitutability of the provider, concentration and dependency, use of material subcontractors, financial viability of the provider, recovery capability, and the potential scale of operational disruption. This should remain illustrative rather than become a mandatory checklist. The objective should

be to improve consistency of risk judgment without recreating the process driven approach the proposed guidance is seeking to correct.

Third, third party risk assessment should be dynamic rather than primarily calendar driven. The proposed guidance appropriately recognizes that changing circumstances may justify reassessment of a relationship. I recommend that the final guidance further encourage event driven reassessment where there is a significant cyber incident, material control failure, regulatory action, financial deterioration, major change in service scope, significant subcontractor change, acquisition, geopolitical exposure, prolonged service interruption, or material change in concentration. Such an approach would permit institutions to devote monitoring resources to changes in actual risk rather than relying principally on uniform annual reassessment cycles.

Fourth, operational resilience should form an integral part of higher risk third party assessment. I support the proposal's recognition that resilience arrangements, alternative providers, segregated data backups, and demonstrated recovery capability may materially reduce the consequences of disruption. For relationships supporting important operations, institutions should consider whether recovery capabilities have been demonstrated through testing rather than relying exclusively on documented continuity plans. Where practical, assessments should consider recovery objectives, service restoration capability, data recovery, dependency mapping, transition options, and the feasibility of exit or substitution during stressed conditions.

Fifth, residual risk acceptance should be clearly connected with governance and risk appetite. The agencies appropriately recognize that eliminating third party risk is neither possible nor economically desirable and that some residual risk may reasonably be accepted. The final guidance could further clarify that material residual risk should be accepted by an authority commensurate with the potential impact of the exposure, particularly where the residual risk approaches or exceeds established risk tolerance. This would preserve management flexibility while ensuring that material risk acceptance represents an informed governance decision rather than the unintended consequence of incomplete due diligence or limited negotiating power.

Finally, I support the agencies' recognition that effective third-party risk management should be considered holistically rather than as a series of isolated lifecycle activities. A strong TPRM framework should connect third party identification, risk assessment, due diligence, contractual safeguards, ongoing monitoring, operational resilience, exit planning, residual risk acceptance and governance into an integrated risk management process. A proportionate framework built on these principles can reduce unnecessary compliance activity while directing attention to the third-party dependencies capable of creating material harm to institutions, customers and the broader financial system.

Thank you for considering these comments.

Bilal Ali Zafar
Risk Management and Governance Professional
RIMS-CRMP| CISA | PMI-RMP | CICA | P3GP®